

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11) 特許番号

第2576385号

(45) 発行日 平成9年(1997)1月29日

(24) 登録日 平成8年(1996)11月7日

(51) Int.Cl. ⁶	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
9/06	5 5 0		9/06	5 5 0 B

請求項の数4 (全 14 頁)

(21) 出願番号	特願平5-270718	(73) 特許権者	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22) 出願日	平成5年(1993)10月28日	(72) 発明者	小倉 直志 東京都港区芝五丁目7番1号 日本電気 株式会社内
(65) 公開番号	特開平7-129473	(74) 代理人	弁理士 京本 直樹 (外2名)
(43) 公開日	平成7年(1995)5月19日	審査官	野仲 松男
		(56) 参考文献	特開 平4-147353 (J P, A) 特開 昭60-167033 (J P, A)

(54) 【発明の名称】 データ保護装置

(57) 【特許請求の範囲】

【請求項1】 1以上のデータ系列の暗号化データを記憶し指定されたアドレスに従って出力する外部記憶装置と、外部記憶装置から暗号化データを入力しデータを復号する復号演算装置と、復号演算装置により復号されたデータを入力し処理するCPUと、CPUから入力されたアドレスを受けて外部記憶装置にアドレスを出力するアドレス制御回路とを備え、

前記復号演算装置は各データ系列の先頭アドレスの暗号化データの復号には初期化パラメータを用いて復号を行い、先頭アドレス以外の暗号化データの復号には直前のアドレスの復号されたデータを基にパラメータを合成して復号を行い、

前記アドレス制御回路は、CPUより入力したアドレスの不連続を検出する検出手段と、前記アドレス不連続検

出により、CPUへの復号データの入力を保留し、不連続となった新たに指定するアドレスの属するデータ系列の先頭アドレスから当該不連続アドレスまで順次暗号化データの読み出しと復号を行わせ、当該不連続アドレスのデータの復号完了後前記保留を解除し、CPUの復号データの入力を再開させる制御手段を有することを特徴とするデータ保護装置。

【請求項2】 前記入力データ系列に対しデータ対データ対応で結合された非線形変換器または線形変換器を有することを特徴とする請求項1記載のデータ保護装置。

【請求項3】 前記制御手段がキャッシュ・コントローラにより構成されることを特徴とする請求項1又は2記載のデータ保護装置およびデータ保護方式。

【請求項4】 前記外部記憶装置へのアドレス信号出力の一部または全部に対して非線形変換または線形変換を

BEST AVAILABLE COPY

施したデータを該初期化パラメータとする手段をさらに有することを特徴とする請求項1、2、又は3記載のデータ保護装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、データ保護装置に関し、特にコンピュータの外部記憶装置に記憶された該コンピュータの実行プログラムに対するデータ保護装置に関する。

【0002】

【従来の技術】従来のコンピュータの外部記憶装置に記憶されたデータの保護装置および保護方式は、図14に示すように外部データ・バス4と内部データ・バス5の間に復号化回路34を有している（例えば、特開昭61-168061号公報参照）。

【0003】図14に示す従来例では、外部記憶装置2にデータを書き込む場合、CPU3は暗号鍵回路36を起動した後、暗号鍵を暗号化回路35にセットする。これにより、CPU3から内部データ・バス5に出力された書き込みデータは暗号化回路35を通過するたびに暗号化されて外部データ・バス4に出力され外部記憶装置2に入力される。CPU3自体のプログラムを書き込む場合には暗号鍵回路36、暗号化回路35を停止して暗号化処理を行わないようにする。

【0004】外部記憶装置から読み出す場合には、暗号鍵回路36を起動した後、暗号鍵を復号化回路34にセットする。これにより、外部記憶装置2から外部データ・バス4上に出力された暗号化データは復号化回路34を通過するたびに元のデータに復号され、内部データ・バス5をとおしてCPU3に入力される。CPU3のプログラムを読み出す場合にはCPU3は命令フェッチ制御線40により復号化回路34の動作を停止し、外部データ・バス4上のデータを、そのまま内部データ・バス5に出力するように制御する。

【0005】暗号化回路35、復号化回路34、暗号鍵回路36の構成は第三者に対して秘密に保持する必要がある。

【0006】以上説明したように図14に示す従来例では、データの暗号化のみでCPU3自体のプログラムの暗号化を行わない。

【0007】CPU3自体のプログラムの暗号化を行う例を図15に示す。外部データ・バス4と内部データ・バス5の間に変換テーブル8を有している。

【0008】変換テーブル8は外部データ・バス4を入力とし、外部データ・バス4の値を非線形変換または線形変換した信号を内部データ・バス5に出力する。変換テーブル8は、外部データ・バス4と同じビット長の非線形演算または線形演算を行う演算器9と任意に設定可能なデータである暗号鍵10とにより構成することができる。例えば4ビット長の場合には図16に示すような

1対1の非線形変換を行うものとする。非線形演算器9の例としては特開平03-254538号公報や特開昭59-45269号公報がある。暗号鍵10を定数とすれば変換テーブル8はあらかじめ各入力信号に対応する出力信号を記憶させた記憶装置により構成することもできる。

【0009】外部記憶装置2には、図7に示すように、あらかじめ図16の逆変換テーブルにより非線形変換された暗号化データが記憶されているものとする。アドレス、データのビット長は説明のためそれぞれ4ビットとする。以降、「」で括まれた各データは特に断らない限り2進数を表すものとする。

【0010】アドレス「0000」の元のデータ「1001」は暗号化データ「1101」に変換される。同様にアドレス「0001」の元のデータ「1110」は暗号化データ「1000」に変換される。ここでアドレス「0000」とアドレス「0011」の元のデータはともに「1001」なので暗号化データもともに「1101」で同じになっている。

【0011】復号時の動作を図18に示す。

【0012】外部記憶装置2は、コンピュータ1から読み出し信号6が入力されると外部アドレス・バス21のアドレスに対応した暗号化データを、外部データ・バス4に出力する。外部データ・バス4の暗号化データは変換テーブル8により非線形変換されて元のデータとなりCPU3に入力される。変換テーブル8の動作は第三者に対して秘密に保持する必要がある。

【0013】1対1変換ではなく1対多の変換を行うデータ秘匿方式の従来例は、図19に示すように変換テーブル8、信号選択回路11、記憶回路14、排他的論理和回路7によりフィードバック・ループを構成する方式を有している。

【0014】変換テーブル8は復号化バス42上の信号を入力とし、非線形変換または線形変換を行った信号を信号選択回路11に出力する。信号選択回路11は変換テーブル8の出力信号と、初期値12と、制御回路43からの選択信号13を入力とし、選択信号13が入力されている場合は初期値12を、それ以外の場合は変換テーブル8の出力信号を、記憶回路14に出力する。初期値12は暗号化バス41と同じビット長の定数である。記憶回路14は、信号選択回路11の出力信号と、制御回路43からのラッチ信号44を入力とし、ラッチ信号44が入力されている場合は信号選択回路11の出力信号を、それ以外の場合は直前のラッチ信号44が入力されていた時に記憶回路14が出力していた信号を、排他的論理和回路7に出力する。排他的論理和回路7は暗号化バス41と記憶回路14からの信号を入力とし、暗号化バス41と記憶回路14の出力信号の排他的論理和演算をした演算結果を復号化バス42に出力する。制御回路43は復号動作開始時に選択信号13を信号選択回路

に出力し、暗号化バス41のデータの各1語を変換する直前ごとにラッチ信号44を記憶回路14に出力する。

【0015】変換テーブル8は、暗号化バス41と同じビット長の非線形演算または線形演算を行う演算器9と任意に設定可能なデータである暗号鍵10とにより構成することができる。例えば4ビット長の場合には図20に示すような1対1の非線形変換を行うものとする。暗号鍵10を定数とすれば変換テーブル8はあらかじめ各入力信号に対応する出力信号を記憶させた記憶装置により構成することもできる。

【0016】暗号化バス41の暗号化データ列の生成手段を図21に示す。本例では、暗号化バスのビット幅として4ビット、変換テーブルとして図20の変換テーブルを用い、元のデータ列の各1語に、時系列順に1、2、3とデータ番号を便宜的に割り当てるものとする。初期値12は定数「1101」とする。

【0017】データ番号1の元のデータ「1001」を暗号化するときには、初期値12「1101」と排他的論理和演算をし、「0100」を暗号化データとして得る。データ番号2の元のデータ「1110」を暗号化するときには、データ番号1の元のデータ「1001」を変換テーブルにより変換した値「1101」と、データ番号2の元のデータ「1110」を排他的論理和演算をし、「0011」を暗号化データとして得る。同様に、データ番号3の元のデータ「0011」を暗号化するときには、データ番号2の元のデータ「1110」を変換テーブルにより変換した値「1000」と、データ番号3の元のデータ「0011」を排他的論理和演算をし、「1011」を暗号化データとして得る。

【0018】つまり n を自然数としデータ番号 n の元のデータ、暗号化データをそれぞれ元のデータ(n)、暗号化データ(n)と表し、変換テーブルによる変数を f で表すと、データ番号 n の元のデータは次の式により暗号化される。

$$\begin{aligned} \text{【0019】暗号化データ}(n) &= \text{元のデータ}(n) \\ &\quad \text{元のデータ}(n) = \text{暗号化データ}(n) \\ &\quad) \dots\dots (\text{式1}) \\ &\quad \text{元のデータ}(0) = \text{初期値} \end{aligned}$$

式1に示すとおり、暗号化データ(n)を元のデータ(n)に復号するには元のデータ($n-1$)が必要だが、元のデータ($n-1$)を得るには元のデータ($n-2$)が必要となる。つまり暗号化データ(n)を復号するには n 以前のすべての元のデータが必要となるため、暗号化バス41上の暗号化データから元のデータを推測することは非常に困難であり暗号強度は高い。

【0026】変換テーブル8の内容は第三者に対して秘密に保持する必要がある。初期値12も秘密に保持することが望ましいが、復号時には元のデータ(1)にしか用いないため、公開しても暗号強度への影響は比較的小さい。したがって初期値12は外部からディップ・スイ

$\text{xor } f(\text{元のデータ}(n-1))$

元のデータ(0) = 初期値

ここで元のデータ(1)と元のデータ(4)はともに「1001」で同じだが、暗号化データはそれぞれ「1000」、「1110」と異なる値に変換されている。

【0020】図19の動作を図22を用いて説明する。

【0021】復号動作開始時には、制御回路43は選択信号13を信号選択回路11に、ラッチ信号44を出力する。これにより記憶回路14の記憶データは初期値12「1101」となる。

【0022】暗号化バス41上の暗号化データ(1)「0100」は、記憶回路14の記憶データ「1101」と排他的論理和回路7により排他的論理和演算され、演算の結果得られる元のデータ(1)である「1001」が復号化バスに出力される。元のデータ(1)である「1001」は変換テーブル8により f (元のデータ(1))「1101」となる。暗号化バス41上の暗号化データ(2)「0011」は、排他的論理和回路7により記憶回路14の記憶データ「1101」と排他的論理和演算され、演算の結果得られる元のデータ(2)である「1110」が復号化バス42に出力される。元のデータ(2)「1110」は変換テーブル8により f (元のデータ(2))「1000」に変換され、信号選択回路11に入力される。

【0023】同様に、暗号化データ(3)の復号化を行う前に制御回路43はラッチ信号44を記憶回路14に出力し、記憶回路14の記憶データは f (元のデータ(2))「1000」となる。暗号化バス41上の暗号化データ(3)「1011」は、排他的論理和回路7により記憶回路14の記憶データ「1000」と排他的論理和演算され、演算の結果得られる元のデータ(3)である「0011」が復号化バス42に出力される。

【0024】つまり、暗号化データ(n)は次の式により元のデータ(n)に復号される。

$$\begin{aligned} \text{【0025】} \\ \text{xor } f(\text{元のデータ}(n-1)) \end{aligned}$$

ッチなどにより設定することも可能である。

【0027】

【発明が解決しようとする課題】図14に示す第一の従来例では、プログラムの秘匿化ができないという問題点があった。また、外部データバス4と内部データ・バス5の間に復号化回路34が挿入されているため、次に説明する図15に示す第二の従来例と同じ問題点を有する。

【0028】図15に示す第二の従来例では、外部データ・バス4と内部データ・バス5の間に交換テーブル8が挿入されているので信号処理に要する時間は交換テーブル8の参照時間が支配的となる。暗号鍵10を定数と

BEST AVAILABLE COPY

し、あらかじめ各入出力信号に対する出力信号を記憶させた記憶装置により変換テーブル8を構成し、変換テーブル8を現在最先端の $0.5\mu\text{m}\sim 0.8\mu\text{m}$ ルールのCMOSプロセスを用いて作成した場合でも、参照時間は少なくとも 20ns 以上は必要である。

【0029】したがって外部記憶装置からの読み出し時間が $30\text{ns}\sim 100\text{ns}$ 程度と高速な、近年の外部記憶装置2とCPU3のシステム構成の場合には、変換テーブル8の参照時間 20ns が外部記憶装置2からの読み出し時間に対して無視できなくなり、第二の従来例によりプログラムの秘匿化を行うにはCPU3にウェイトをかける、または動作周波数を下げなければならず、結果としてコンピュータ1の性能を大きく低下させるという欠点があった。

【0030】また、外部データ・バス4上の暗号化データと、内部データ・バス5上の元のデータが1対1に対応しているため、プログラムの秘匿化の場合、各命令の使用頻度に差があることを利用すると、第三者が外部データ・バス4上の暗号化データから元のデータを推測することは、比較的容易である。例えば暗号化データ列中で最も出現頻度の大きい暗号化データが、転送命令に対応するだろうと推測することができる。したがって、外部データ・バス4が8ビット幅程度のコンピュータ1の場合、すべてを推測する計算量は非常に小さく暗号強度は低いという問題点があった。

【0031】図19に示した第三の従来例の場合には、1対多への変換であり第二の従来例の問題点はない。暗号化バス41と復号化バス42の間には排他的論理和回路7が挿入されているのみであり、排他的論理和回路7の遅延時間は現在の $0.5\mu\text{m}\sim 0.8\mu\text{m}$ ルールのCMOSプロセスで構成した場合数 ns 程度であり、近年の高速な外部記憶装置2の読み出し時間に対しても無視できる程度である。また、元のデータ(n)を得るために変換テーブル8に暗号化データ(n)を入力する第二の従来例と異なり、第三の従来例では元のデータ(n)を得るために変換テーブル8に入力するのは元のデータ(n-1)である。したがって変換テーブル8の出力信号を参照するのは変換テーブル8に入力してから1読み出し周期後となり、変換テーブル8の遅延時間が外部記憶装置2からの読み出し動作に影響を与えることはなく、第二の従来例のようにCPU3の性能を低下させることもない。

【0032】ただし、第三の従来例の場合には、式1に示すとおり、暗号化データ(n)を元のデータ(n)に復号するには元のデータ(n-1)が必要だが、元のデータ(n-1)を得るには元のデータ(n-2)が必要となる。つまり例えば図22の暗号化データ(7)を復号するには暗号化データ(1)から暗号化データ(6)までのすべての暗号化データが、データ番号の順番で復号されていなければならない。

【0033】これに対して、ほとんどのプログラムは分岐命令を有しているため、外部記憶装置から読み出されるデータはアドレスの順番で読み出されるとは限らないため、第三の実施例を適用することは非常に困難である。

【0034】例えば図22のデータ番号をアドレスとみなし、アドレス4の元のデータがアドレス7への分岐命令の場合、アドレス1、2、3、4と順番に暗号化データを復号した後、アドレス5の暗号化データではなくアドレス7の暗号化データを復号しようとするが、アドレス6の元のデータが記憶回路14に記憶されていないため正しく復号することができない。

【0035】したがって第三の実施例は、コンピュータのプログラムの秘匿化に適用することは非常に困難であるという問題点を有する。

【0036】

【課題を解決するための手段】本発明のデータ保護装置およびデータ保護方式は、1以上のデータ系列の暗号化データを記憶し指定されたアドレスに従って出力する外部記憶装置と、外部記憶装置から暗号化データを入力しデータを復号する復号演算装置と、復号演算装置により復号されたデータを入力し処理するCPUと、CPUから入力されたアドレスを受けて外部記憶装置にアドレスを出力するアドレス制御回路を備え、前記復号演算装置は各データ系列の先頭アドレスの暗号化データの復号には初期化パラメータを用いて復号を行い、先頭アドレス以外の暗号化データの復号には直前のアドレスの復号されたデータを基にパラメータを合成して復号を行い、前記アドレス制御回路は、CPUより入力したアドレスの不連続を検出する検出手段と、前記アドレス不連続検出により、CPUへの復号データの入力を保留し、不連続となった新たに指定するアドレスの属するデータ系列の先頭アドレスから当該不連続アドレスまで順次暗号化データの読み出しと復号を行わしめ、当該不連続アドレスのデータの復号完了後前記保留を解除し、CPUの復号データの入力を再開させる制御手段を有する。

【0037】

【実施例】次に本発明について図面を参照して説明する。

【0038】図1は本発明の第一の実施例の構成を示すブロック図である。

【0039】変換テーブル8は内部データ・バス5上の信号を入力とし、非線形変換または線形変換を行った信号を信号選択回路11に出力する。信号選択回路11は変換テーブル8の出力信号と、初期値12と、アドレス制御回路15からの選択信号13を入力とし、選択信号13が入力されている場合は初期値12を、それ以外の場合は変換テーブル8の出力信号を、記憶回路14に出力する。初期値12は外部データ・バス4と同じビット長の定数である。記憶回路14は、信号選択回路11の

BEST AVAILABLE COPY

出力信号と、アドレス制御回路15からの読み出し信号6を入力とし、読み出し信号6が有効のときには信号選択回路11の出力信号を、読み出し信号6が無効のときには直前の読み出し信号6が有効のときに記憶回路14が出力していた信号を、排他的論理和回路7に出力する。排他的論理和回路7は外部データ・バス4と記憶回路14からの信号を入力とし、外部データ・バス4と記憶回路14の出力信号の排他的論理和演算をした演算結果を内部データ・バス5に出力する。アドレス制御回路15はCPU3からの内部アドレス・バス16と内部読み出し信号17と分岐信号18と読み出しクロック信号19を入力とし、外部記憶回路2に外部アドレス・バス21と読み出し信号6を出力し、記憶回路14に読み出し信号6を出力し、CPU3に対しBUSY信号3を出力する。

【0040】外部記憶装置2には一つまたは複数のデータ系列が暗号化されてあらかじめ記憶されている。各データ系列長は等しく、ここでは4とする。また各データ系列の先頭データのアドレスのうち、データ系列長に相当する下位ビットは互いに等しいものとする。ここではデータ系列長を4としたので下位2ビットは互いに等しいことになり、ここでは「00」とする。

【0041】CPU3は外部記憶装置2からのデータの1語読み出し動作ごとに内部アドレス・バス16と内部読み出し信号17を出力し、分岐命令を実行して内部アドレス・バス16が不連続になると分岐信号18を出力し、内部読み出し信号17に周期も等しく読み出し動作保留中も出力される読み出しクロック信号19を出力する。また、CPU3はBUSY信号20が有効の時には外部記憶装置2に対する読み出し動作を保留する。

【0042】アドレス制御回路15は内部アドレス・バス16と外部アドレス・バスが等しくない期間BUSY信号20を出力する。

【0043】分岐信号18が入力されると、外部記憶装置2に記憶されている暗号データ系列の系列長に相当するビット数の外部アドレス・バス21の下位ビット数をその暗号データ系列の先頭アドレスの系列長に相当する下位ビットに変更して外部アドレス・バス21に出力するとともに選択信号13を出力する。ここでは分岐信号18が入力されるごとに外部アドレス・バス21の下位2ビットを「00」に変更する。また、内部読み出し信号17または、BUSY信号20が有効の間は読み出しクロック信号19を読み出し信号6として出力する。これによりCPU3が読み出し動作を保留している期間も外部記憶装置2からは暗号データ系列が読み出されることになる。

【0044】変換テーブル8は、外部データ・バス4と同じビット幅の非線形演算または線形演算を行う演算器9と任意に設定可能なデータである暗号鍵10とにより構成することができる。例えば4ビット幅の場合には図

20に示すような1対1の非線形変換を行うものとする。暗号鍵10を定数とすれば変換テーブル8はあらかじめ各入力信号に対応する出力信号を記憶させた記憶装置により構成することもできる。

【0045】変換テーブル8、信号選択回路11、初期値12、選択信号13、記憶回路14、排他的論理和回路7の動作は第三の従来例と同様である。

【0046】アドレス制御回路15の一構成例を図2に、信号波形図を図3に示す。ここでは暗号データ系列の系列長は16、各系列の先頭アドレスの下位4ビットは「0000」とし、外部アドレス・バス21のビット幅は16とする。

【0047】4ビット・カウンタ22にはリセット信号として分岐信号18が、カウント・読み出しクロック信号として読み出し信号6が入力され、そのカウンタ出力信号27を4ビット・セレクト24に出力する。4ビット・セレクト24は内部アドレス・バス16の下位4ビットと、カウンタ出力信号27とBUSY信号20を入力とし、BUSY信号20が有効のときにはカウンタ出力信号27を、BUSY信号20が無効の時には内部アドレス・バス16の下位4ビットを外部アドレス・バスの下位4ビットに出力する。比較回路23は内部アドレス・バス16の下位4ビットとカウンタ出力信号27を入力とし、2つの入力信号が等しくない場合BUSY信号を出力する。0判定回路25はカウンタ出力信号27を入力とし、入力が0の場合には選択信号13を出力する。

【0048】1ビット・セレクト26は内部読み出し信号17と読み出しクロック信号19とBUSY信号20を入力とし、BUSY信号20が有効の時には読み出しクロック信号19を、無効の時には内部読み出し信号17を外部読み出し信号6に出力する。

【0049】図3の信号波形図を用いてアドレス制御回路15の動作を説明する。以降、特に断らない限りHで終わる数は16進数を表すものとする。

【0050】CPU3がアドレス1242Hで分岐命令を実行し、アドレス3432Hに分岐した場合を例として説明する。

【0051】アドレス1242Hまでは順次連続してデータ系列を読み込むため分岐信号18は入力されず、カウンタ出力信号27と内部アドレス・バス16の下位ビットは一致している。アドレス1240Hになると新しい暗号データ系列に移行するため選択信号13を出力する。

【0052】アドレス1242Hからアドレス3432Hに分岐するとCPU3から分岐信号が入力され4ビット・カウンタ22が0にリセットされ選択信号13が出力されるとともに、カウンタ出力信号27が内部アドレス・バス16の下位4ビットと一致なくなるためBUSY信号20が発生する。外部アドレス・バス21は3

BEST AVAILABLE COPY

430Hとなり、以後は読み出し信号6により外部アドレス・バス21は3431H、3432Hと変化していく。このとき外部記憶装置2から暗号化データ系列が読み出されて行くが、3430H、3431HのときにはBUSY信号20がCPU3に入力されているため内部データ・バス5の値は読み込まれない。以降外部アドレス・バス21が3432Hとなるとカウンタ出力信号27と内部アドレス・バス16の下位4ビットが一致するためBUSY信号20が無効となりCPUは読み出し動作を再開する。

【0053】ここで、アドレス3432Hでなくアドレス3430Hに分岐する場合には、カウンタ出力信号27と内部アドレス・バス16の下位4ビットが一致するためにBUSY信号20は発生せず、選択信号13のみが出力されることになる。

【0054】暗号化データ系列の生成手順を図4に示す。図4の例では、アドレス、データのビット幅はともに4ビットとする。変換テーブルは図5の変換テーブルを用いる。初期値12は定数「1101」とする。また、暗号データ系列の系列長は4、各系列の先頭アドレスの下位2ビットは「00」とする。

【0055】図4のとおり、アドレスの下位2ビットが「00」になるたびに元のデータ系列と排他的論理和をとるデータを初期値「1101」に変更することのみが第三の従来例と異なり、系列長が4の暗号データ系列を生成する動作は従来例と同様である。

【0056】本発明の第一の実施例の分岐命令を実行しない場合の動作を図6～図8を用いて説明する。図6は分岐命令を実行しない場合の信号波形図であり、図8はこのときのデータの流れを示す図である。

【0057】暗号化データ系列の生成時の動作の説明の場合と同様、アドレス、データのビット幅はともに4ビットとする。変換テーブルとして図7の変換テーブルを用いる。初期値12は定数「1101」とする。また、暗号データ系列の系列長は4、各系列の先頭アドレスの下位2ビットは「00」とする。

【0058】分岐命令を実行しないため分岐信号18は発生せず、CPU3が出力する内部アドレス・バス16とアドレス制御回路15が出力する外部アドレス・バス21の内容は常に一致している。このためアドレス制御回路15はBUSY信号20を出力せず、CPU3は読み出し動作を保留せず内部データ・バス5上の元のデータ系列を内部読み出し信号17に応じて読み込んでいく。外部アドレス・バス21の下位2ビットが「00」になるごとに選択信号13を信号選択回路13に出力し、内部データ・バス5と排他的論理和をとるデータを初期値「1101」に変更する。

【0059】図8より系列長4の各データ系列の中のデータの流れは第三の従来例と同様であり、各暗号データ系列がすべて正しく元のデータに復号されることが分か

る。

【0060】本発明の第一の実施例の分岐命令を伴う場合の動作を図9～図11を用いて説明する。図9は分岐命令を伴う場合の信号波形図であり、図11はこのときのデータの流れを示す図である。ここでは、アドレス「0000」からアドレス「0010」まで順次外部記憶装置2から読み出し、アドレス「0010」で分岐命令を実行する結果アドレス「0110」に分岐する場合を例に説明する。

【0061】暗号化データ系列の生成時の動作の説明の場合と同様、アドレス、データのビット幅はともに4ビットとする。変換テーブルとして図10の変換テーブルを用い、初期値12は定数「1101」とする。また、暗号データ系列の系列長は4、各系列の先頭アドレスの下位2ビットは「00」とする。

【0062】アドレス「0000」からアドレス「0010」までは分岐命令を伴わずに順次読み出すため、分岐信号18が発生せずCPU3が出力する内部アドレス・バス16とアドレス制御回路15が出力する外部アドレス・バス21の内容は常に一致している。図11からこの場合のデータの流れは第三の実施例と同じであり、暗号化データが元のデータに正しく復号されていることが分かる。

【0063】CPU3は内部データ・バス5からアドレス「0010」の元のデータを読み込んだ後アドレス「0110」への分岐命令を実行するため、分岐信号18を出力し、内部アドレス・バス16に「0110」を出力し、外部記憶装置2からアドレス「0110」の暗号化データを読み出そうとする。しかし、分岐信号18により外部アドレス・バス21の下位2ビットは「00」となるため、アドレス制御回路15は外部アドレス・バス21に「0100」を出力するとともに信号選択回路11に選択信号13を出力する。また内部アドレス・バス16と外部アドレス・バス21が一致しないのでアドレス制御回路15がCPU3にBUSY信号20を出力するため、CPU3は読み出し動作を保留する。

【0064】選択信号13によって記憶回路14の記憶データが演算器8の出力ではなく初期値12となっているため、下位2ビットが「00」から始まる新しい暗号データ系列の先頭データであるところのアドレス「0100」の暗号化データは排他的論理和回路7により正しく元のデータに復号され内部データ・バスに出力される。

【0065】この後、CPU3は読み出し動作を保留状態だが、アドレス制御回路15は読み出しクロック信号19に従って外部アドレス・バス21に「0101」と読み出し信号4を出力し、外部記憶装置2からの読み出し動作を続行する。

【0066】CPU3が読み出し動作を保留している間に内部データ・バス7上に出力されたアドレス「010

BEST AVAILABLE COPY

0」の元のデータと、アドレス「0101」の元のデータは、CPU3の動作に影響を与えることはなく、次の暗号化データを復号するために演算器8に入力されるだけである。

【0067】アドレス制御回路15が読み出しクロック信号19に従い外部アドレス・バス21に「0110」を出力すると、外部アドレス・バス21と内部アドレス・バス16が一致するためBUSY信号20が無効となりCPU3は読み出し動作を再開する。

【0068】ここで分岐命令による分岐先アドレス「0110」の暗号化データは、すでにアドレス「0101」の暗号化データが元のデータに復号されているために、第三の従来例の場合と異なり、正しく元のデータに復号されて内部データ・バス5に出力され、読み出し動作を再開したCPU3に読み込まれる。

【0069】以降の動作は次の分岐命令を実行するまでの間、図6～図8で前述した動作と同様である。

【0070】以上説明した通り、本発明のデータ保護回路は分岐処理を伴う場合でも、従来例と異なり、暗号化データ系列を元のデータ系列に正しく復号することができる。

【0071】図12は本発明の第二の実施例の構成を示すブロック図である。

【0072】本実施例では、アドレス制御回路15の代わりにキャッシュ・コントローラ28とキャッシュ・メモリ29とCPUデータ・バス30を有しており、その他は、第一の実施例と同様である。キャッシュ・コントローラ28はフェッチ・パイパス・リプレース動作を行わないものとする。

【0073】外部記憶装置2には一つまたは複数のデータ系列が暗号化されてあらかじめ記憶されている。各データ系列長は等しく、また各系列の先頭アドレスはデータ系列長に相当する下位ビット数だけ等しい。

【0074】キャッシュ・コントローラ28は、CPU3からの内部アドレス・バス16、内部読み出し信号17、分岐信号18、読み出しクロック信号19を入力とし、外部アドレス・バス21と読み出し信号6とCPUデータ・バス30と選択信号13を出力する。またキャッシュ・メモリ29に対して任意に読み書きが可能である。CPU3が読み出し動作を行い内部アドレス・バス16に読み出しアドレスを出力すると、キャッシュ・コントローラ28はその読み出しアドレスの元のデータがキャッシュ・メモリ29に記憶されているかどうかを判別し、記憶されている場合には該当する元のデータをCPUデータ・バス30に出力する。キャッシュ・メモリ29に記憶されていない場合、キャッシュ・コントローラ28は選択信号13を出力するとともに外部記憶装置21から該当アドレスを含む暗号化データ系列をその系列の先頭アドレスからその系列の最終アドレスまで読み出す動作を行い、その間BUSY信号20を出力してC

PU3の読み出し動作を停止させる。このとき外部記憶装置2から読み出された暗号化データ系列は第一の従来例と同様に正しく元のデータ系列に復号されて内部データ・バス5に出力され、キャッシュ・コントローラ28によって順次キャッシュ・メモリ29に書き込まれる。キャッシュ・コントローラ28は該当アドレスを含む暗号化データ系列をその最終アドレスまで復号してキャッシュ・メモリ29に書き込むと、BUSY信号20を無効にしてCPU3の読み出し動作を再開させる。このときは内部アドレス・バス16上のアドレスに対応する元のデータがキャッシュ・メモリ29に記憶されているので、キャッシュ・コントローラ28は該当データをキャッシュ・メモリから読み出し、CPUデータ・バス30に出力する。

【0075】以上説明したように、キャッシュ・メモリ29を有するコンピュータ1では、キャッシュ・コントローラ28の動作を活用することによりアドレス制御回路15を特に有さなくとも本発明のデータ保護装置を構成することができる。

【0076】図13は本発明の第三の実施例の構成を示すブロック図である。

【0077】本実施例は、初期値12の替わりに第2の変換テーブル31を有する他は、第一の実施例と同様である。

【0078】第2の変換テーブル31は外部アドレス・バス21上の信号を入力とし、非線形変換または線形変換を行った信号を信号選択回路11に出力する。

【0079】第2の変換テーブル8は、外部データ・バス4と同じビット幅の出力を有する非線形演算または線形演算を行う第2の演算器32と任意に設定可能なデータである第2の暗号鍵33とにより構成することができる。第2の暗号鍵33を定数とすれば第2の変換テーブル31はあらかじめ各入力信号に対応する出力信号を記憶させた記憶装置により構成することもできる。

【0080】外部記憶装置2に記憶された各暗号化データ系列の先頭データは、その先頭データのアドレスを第2の変換テーブル31に入力したときの出力信号により暗号化されているものとする。

【0081】各暗号化データ系列の先頭アドレスはそれぞれ異なるため、各暗号化データ系列の先頭データはそれぞれ異なる信号により暗号化されることになる。

【0082】第三の実施例の動作は、信号選択回路11が選択信号13が入力されている場合に出力する信号が、初期値12ではなく、外部アドレス・バス21を入力とした第2の変換テーブル31の出力信号であることが異なる他は、第一の実施例と同様である。

【0083】第一の実施例、第二の実施例では、各暗号化データ系列の先頭データは一定の初期値12と排他的論理和演算をとることにより暗号化、復号化されていたため、各暗号化データ系列の先頭データの暗号化データ

BEST AVAILABLE COPY

と元のデータの間には従来例2と同様に1対1対応が存在する。このため多数の暗号化データ系列を有する外部記憶装置2の場合には暗号強度が低下する一因になり得る。

【0084】しかし、第三の実施例では各暗号化データ系列の先頭データは、それぞれ異なる先頭アドレスを入力とした第2の変換テーブル31の出力信号で排他的論理和されるため、各暗号化データ系列の先頭データの暗号化データと元のデータの間には1対1対応がなく、1対多対応となり、第一の実施例、第二の実施例に比べて暗号強度を向上させることができる。

【0085】

【発明の効果】本発明による効用として次のものが挙げられる。

【0086】第一に、本発明の解読のための計算量と、第一の従来例および第二の従来例の解読のための計算量の比率は少なくとも次の値以上となる。

【0087】従来例に対する解読計算量の比率＝（2の（外部データ・バス4のビット幅）乗）の（暗号化データ系列長－1）乗

例えば外部データ・バス4のビット幅が8で、暗号化データ系列長が4の場合、暗号強度は 10^7 倍以上となり実用上解読される心配はない。

【0088】第二に、本発明では、外部データ・バス4と内部データ・バス5の間には排他的論理和回路7を一段を挿入するのみであり、外部データ・バス4と内部データ・バス5の間の遅延は無視できるほど小さく、動作クロックが50MHz以上の高速なCPU3に適用することも容易である。

【0089】従来例では、外部データ・バス4と内部データ・バス5の間に変換テーブル8が挿入されていたため遅延時間が非常に大きく、せいぜい動作クロックが5MHz程度のCPU3にしか適用できなかった。

【0090】第三に、本発明のデータ保護装置の回路規模は、従来例と比べてほとんど増加していない。暗号鍵10、第2の暗号鍵33を定数としてあらかじめ変換テーブル8、第2の変換テーブル31を用意すれば、8ビット・データ・バスの場合、512バイトのROMとおよそ1000ゲート程度で構成できる。

【0091】暗号強度の観点から比較すると、本発明と同程度の暗号強度を得るために、第2の従来例の変換テーブル8に特開平03-254538号公報または特公昭59-45269号公報を用いた場合には、構成に10万ゲート以上が必要である。

【0092】以上説明したとおり、本発明を用いれば外部記憶装置の安全かつ高速なデータ保護装置を安価に構成することができる。

【図面の簡単な説明】

【図1】本発明の一実施例の構成を示すブロック図。

【図2】図1に示すアドレス制御回路のブロック図。

【図3】図2に示すアドレス制御回路の動作を説明する信号波形図。

【図4】図1に示す外部記憶装置に記憶されるデータの暗号処理の動作を説明する流れ図。

【図5】図4で示した変換テーブルの一例。

【図6】図1に示す実施例の分岐命令を実行しない場合の動作を説明する信号波形図。

【図7】図6の説明で用いる図1に示す変換テーブルの一例。

【図8】図6の説明を補足するための流れ図。

【図9】図1に示す実施例の分岐命令を実行した場合の動作を説明する信号波形図。

【図10】図9の説明で用いる図1に示す変換テーブルの一例。

【図11】図9の説明を補足するための流れ図。

【図12】本発明の第二の実施例の構成を示すブロック図。

【図13】本発明の第三の実施例の構成を示すブロック図。

【図14】従来例の構成を示すブロック図。

【図15】第二の従来例の構成を示すブロック図。

【図16】図15の説明で用いる図15に示す変換テーブルの一例。

【図17】図15に示す外部記憶装置に記憶されているデータの暗号処理の動作を説明する流れ図。

【図18】図15の動作を説明する流れ図。

【図19】第三の従来例の構成を示すブロック図。

【図20】図19の説明に用いる図11aに示す変換テーブルの一例。

【図21】図19に示す暗号化バス上の暗号化データの作成手順を示す流れ図。

【図22】図19の動作を説明する流れ図。

【符号の説明】

- 1 コンピュータ
- 2 外部記憶装置
- 3 CPU
- 4 外部データ・バス
- 5 内部データ・バス
- 6 読み出し信号
- 7 排他的論理和回路
- 8 変換テーブル
- 9 演算器
- 10 暗号鍵
- 11 信号選択回路
- 12 初期値
- 13 選択信号
- 14 記憶回路
- 15 アドレス制御回路
- 16 内部アドレス・バス
- 17 内部読み出し信号

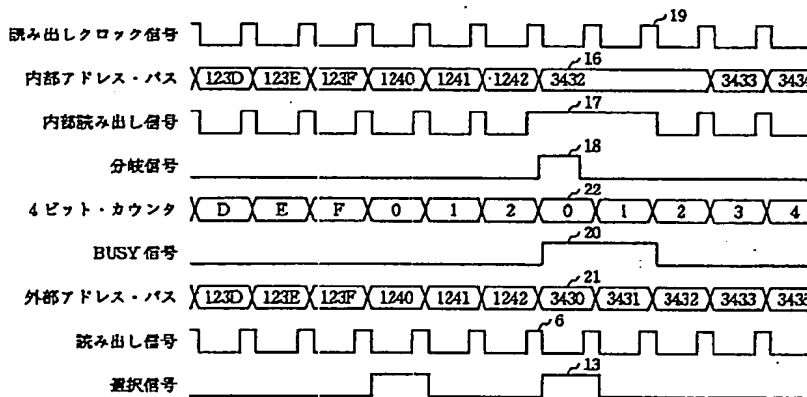
(9)

特許2576385

- | | | | |
|----|--------------|-------|-----------|
| 17 | | | |
| 18 | 分岐信号 | * 32 | 第二の演算器 |
| 19 | 読み出しクロック信号 | 33 | 第二の暗号鍵 |
| 20 | BUSY信号 | 34 | 復号化回路 |
| 21 | 外部アドレス・バス | 35 | 暗号化回路 |
| 22 | 4ビット・カウンタ | 36 | 暗号鍵回路 |
| 23 | 比較回路 | 37 | 暗号鍵回路制御線 |
| 24 | 1ビット・セレクタ | 38 | 暗号化回路起動線 |
| 25 | 0判定回路 | 39 | 復号化回路起動線 |
| 26 | 1ビット・セレクタ | 40 | 命令フェッチ制御線 |
| 27 | カウンタ出力信号 | 10 41 | 暗号化バス |
| 28 | キャッシュ・コントローラ | 42 | 復号化バス |
| 29 | キャッシュ・メモリ | 43 | 制御回路 |
| 30 | CPUデータ・バス | 44 | トリガ信号 |
| 31 | 第二の変換テーブル | * | |

【図3】

【図5】



変換テーブル

0000→1010	1000→1011
0001→0101	1001→1101
0010→0011	1010→0100
0011→0111	1011→1001
0100→0010	1100→0000
0101→1110	1101→0110
0110→1100	1110→1000
0111→1111	1111→0001

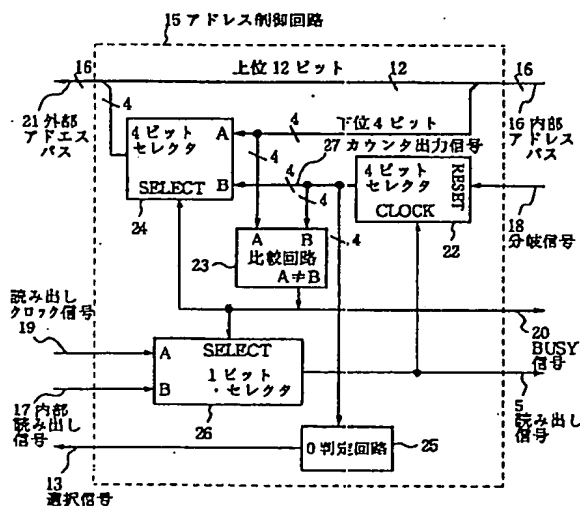
【図10】

変換テーブル

0000→1010	1000→1011
0001→0101	1001→1101
0010→0011	1010→0100
0011→0111	1011→1001
0100→0010	1100→0000
0101→1110	1101→0110
0110→1100	1110→1000
0111→1111	1111→0001

【図2】

【図7】



変換テーブル

0000→1010	1000→1011
0001→0101	1001→1101
0010→0011	1010→0100
0011→0111	1011→1001
0100→0010	1100→0000
0101→1110	1101→0110
0110→1100	1110→1000
0111→1111	1111→0001

【図20】

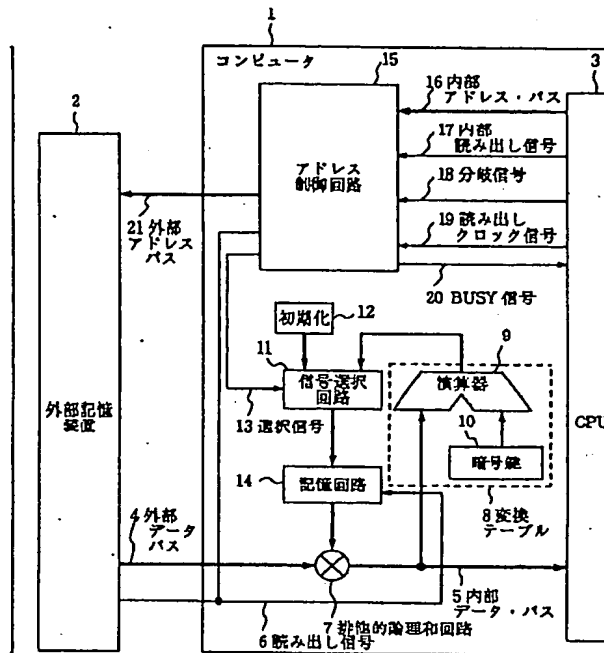
変換テーブル

0000→1010	1000→1011
0001→0101	1001→1101
0010→0011	1010→0100
0011→0111	1011→1001
0100→0010	1100→0000
0101→1110	1101→0110
0110→1100	1110→1000
0111→1111	1111→0001

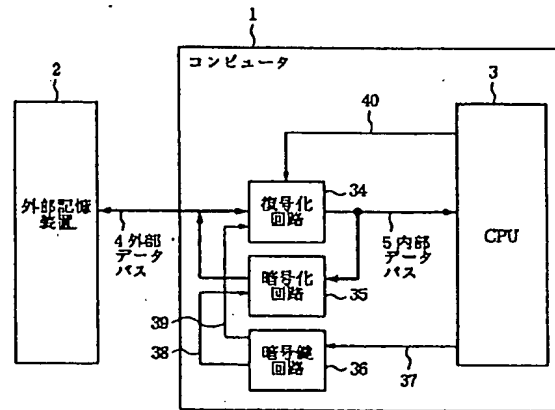
(10)

特許2576385

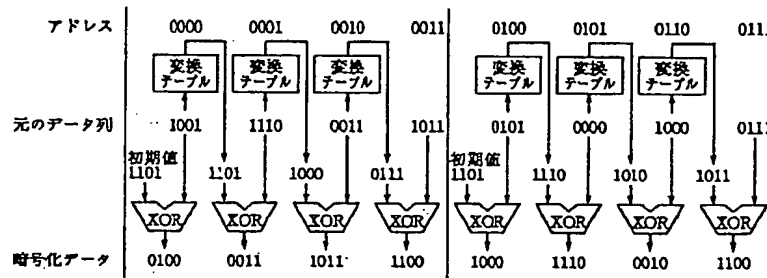
【図1】



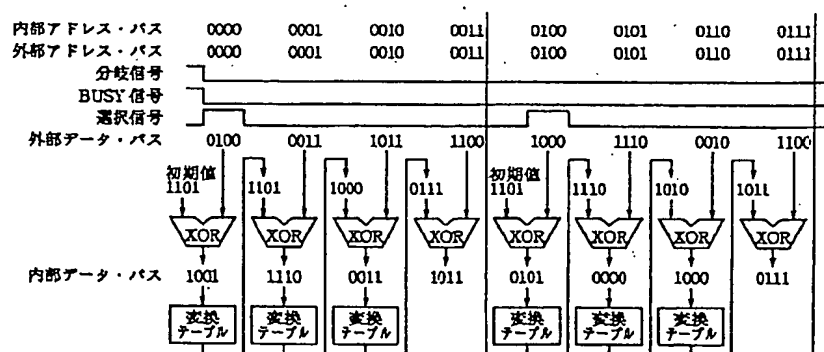
【図14】



【図4】



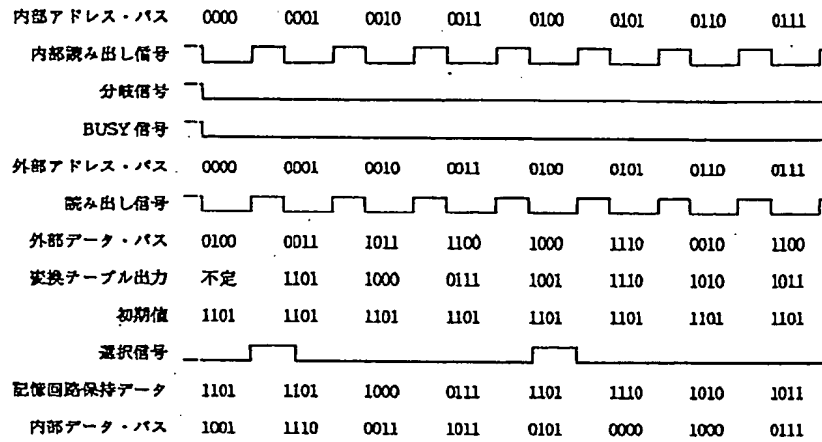
【図8】



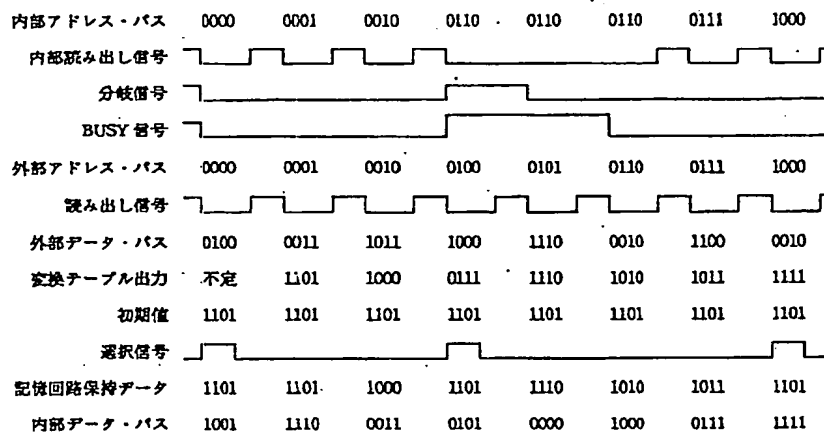
(11)

特許2576385

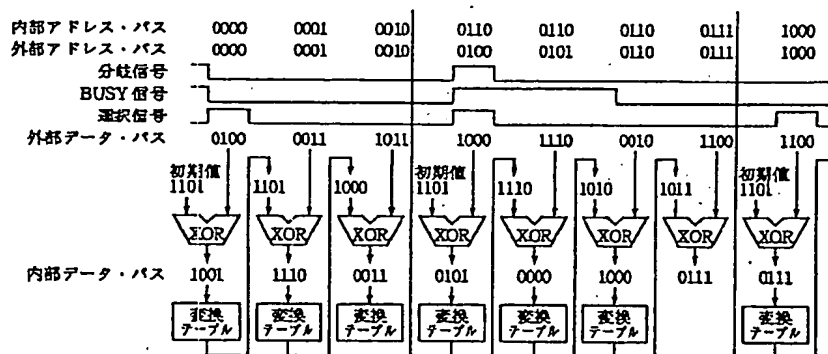
【図6】



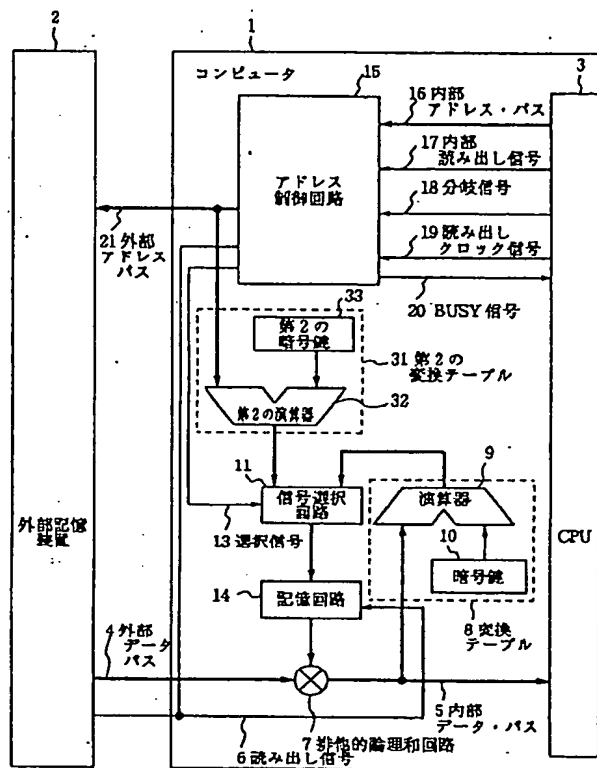
【図9】



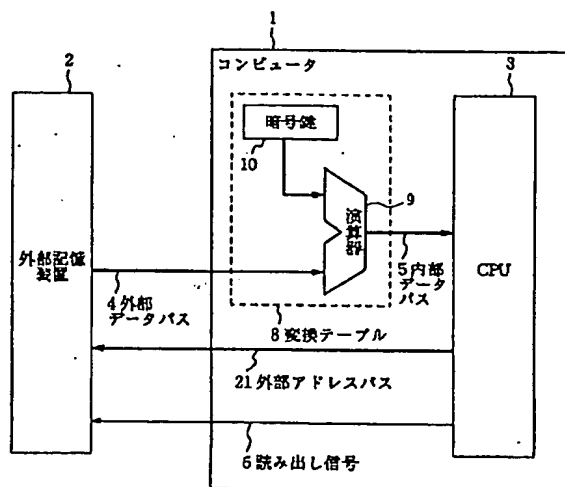
【図11】



【圖 13】



【圖 16】



0000→1010	1000→1011
0001→0101	1001→1101
0010→0011	1010→0100
0011→0111	1011→1001
0100→0010	1100→0000
0101→1110	1101→0110
0110→1100	1110→1000
0111→1111	1111→0001

0000→1100	1000→1101
0001→1111	1001→1011
0010→0100	1010→0000
0011→1001	1011→1000
0100→1010	1100→0110
0101→0001	1101→1001
0110→1101	1110→0101
0111→0011	1111→0111

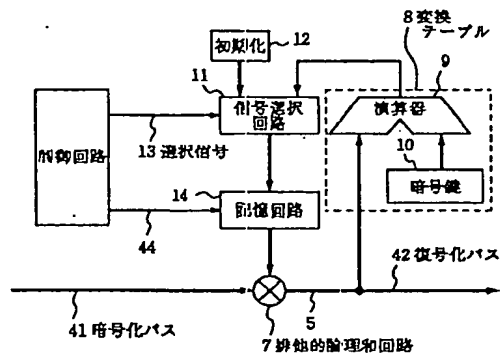
【図17】

アドレス	0000	0001	0010	0011	0100	0101	0110	0111
元のデータ列	1001	1110	0011	1001	0101	0000	1000	0111
	↓	↓	↓	↓	↓	↓	↓	↓
	逆変換 テーブル	逆変換 テーブル	逆変換 テーブル	逆変換 テーブル	逆変換 テーブル	逆変換 テーブル	逆変換 テーブル	逆変換 テーブル
	↓	↓	↓	↓	↓	↓	↓	↓
暗号化データ	1101	1000	0111	1101	1110	1010	1011	1111

【図18】

アドレス	0000	0001	0010	0011	0100	0101	0110	0111
暗号化データ	1101	1000	0111	1101	1110	1010	1011	1111
	↓	↓	↓	↓	↓	↓	↓	↓
	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル
	↓	↓	↓	↓	↓	↓	↓	↓
元のデータ列	1001	1110	0011	1001	0101	0000	1000	0111

【図19】



【図21】

データ番号	1	2	3	4	5	6	7	8
	↓	↓	↓	↓	↓	↓	↓	↓
	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル	変換 テーブル
	↓	↓	↓	↓	↓	↓	↓	↓
元のデータ列	1001	1110	0011	1001	0101	0000	1000	0111
	↓	↓	↓	↓	↓	↓	↓	↓
	初期値 1101	1101	1000	0111	1101	1110	1010	1011
	↓	↓	↓	↓	↓	↓	↓	↓
	XOR	XOR	XOR	XOR	XOR	XOR	XOR	XOR
	↓	↓	↓	↓	↓	↓	↓	↓
暗号化データ	0100	0011	1011	1110	1000	1110	0010	1100

(14)

特許2576385

【図22】

